User-Side Wi-Fi Evil Twin Attack Detection Using Random Wireless Channel Monitoring

Omar Nakhila
Dept. of Electrical & Computer Engineering
University of Central Florida
Orlando FL, USA
omar_hachum@knights.ucf.edu

Cliff Zou
Dept. of Computer Science
University of Central Florida
Orlando FL, USA
czou@cs.ucf.edu

***Abstract*—Free open wireless Internet access is a complimentary Wi-Fi service offered by most coffee shops, fast food restaurants and airports to their customers. For ease of access, these Wi-Fi networks are inherently insecure where no authentication/encryption is used to protect customers wireless data. An attacker can easily deceive a wireless customer (WC) by setting up a rogue access point (RAP) impersonating the legitimate access point (LAP). The WC connecting to the RAP becomes an easy target to the Man-In-the-Middle Attack (MIMA) and data traffic snooping. In this paper, we present a real-time client-side detection scheme to detect evil twin attack (ETA) when the attacker relies on the LAP to direct WC data to the Internet. The WC can detect ETA by monitoring multiple Wi-Fi channels in a random order looking for specific data packets sent by a dedicated sever on the Internet. Once an ETA is detected, our scheme can clearly identify whether a specific AP is a LAP or a RAP. The effectiveness of the proposed detection method was mathematically modeled, prototyped and evaluated in real life environment with a detection rate approximates to 100%.**

***Index Terms*—WLANs Security, Evil twin attack, Open WiFi-Hop.**

I. Introduction

Wireless networks are the gateway to the Internet for smart phones, mobile PCs and tablets. The growth and use of wireless devices has increased data traffic on cellular networks [1]. Some business such as coffee shops, fast food restaurants and airports offer free Wi-Fi services to their customers. Besides from offloading data traffic from cellular networks [2], the use of Wi-Fi provides a fast and budget friendly alternative to wireless customer (WC) when it comes to accessing the Internet [3]. However, for ease of access, these Wi-Fi networks provide no security in terms of authentication or encryption. When a WC wants to access a Wi-Fi network, he/she must agree on the "Public Wi-Fi Access Terms and Conditions" in which the Wi-Fi provider assumes no responsibility for the security/privacy of the WC's information [4].

Insecure Wi-Fi networks provide a tempting environment for attackers to initiate many attacks, one of them is called Evil Twin Attack (ETA) as illustrated in Figure 1. ETA refers to a Wi-Fi rogue access point (RAP) impersonating a legitimate access point (LAP) to eavesdrop WC's Wi-Fi data [3][4][5][6][7][8]. Since a Wi-Fi network can only be recognized by its SSID and MAC address, the attacker can set up a RAP with the same SSID of the LAP. Furthermore, the attacker's RAP may have better and more powerful signal than the LAP which will trick the WC to connect to it first [9]. After the WC connects to the RAP, the attacker can snoop the WC data traffic and start the man-in-the-middle attack (MIMA).

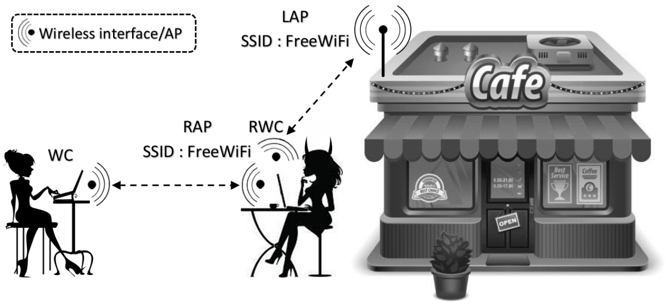

Fig. 1. Evil twin attack using single ISP gateway (WC: wireless customer; RAP: rouge access point; RWC: rogue wireless customer; LAP: legitimate access point)

Once the WC is connected to the RAP, the attacker will have two options to direct WC data traffic to the Internet. First, the attacker can use a Wi-Fi interface card and connect to the LAP as a rogue wireless customer (RWC). The attacker will use the Wi-Fi interface card to pass the WC traffic to the Internet. Both LAP and RAP will use the same ISP gateway as shown in Figure 1. Hence, we call this attack option as ETA using single ISP gateway.

The attacker has another option to avoid connecting to the LAP. Due to the increase in Internet access speed of mobile broadband connections, such as 4G Long Term Evolution (LTE) or WiMAX, the attacker can use his/her own cellular broadband link to connect the WC to the Internet [5][6][8]. In this scenario, the attacker will be in between the RAP and her broadband connection. We call this attack option as ETA using different ISP gateways.

In this paper, we will focus on ETA using single ISP gateway. Our ETA detection technique contributed to the Wi-Fi security by:

- The proposed ETA detection is a real time procedure that examines all nearby access points (APs) in a parallel manner. At the end of the detection procedure, each AP is marked as either LAP or RAP.

- The proposed ETA detection will monitor multiple Wi-Fi channels in random order looking for special wireless frames. These frames are sent from a dedicated public server on the Internet. By capturing these special wireless frames, WC can detect the RAP instantaneously.
- Our ETA detection is a client side solution which makes it more preferable than the network administrator side solutions [6][7] since a WC can ensure his/her security without any assistance from network administrators. Also, the WC does not need to have any information about the Wi-Fi network configuration or any trained data or Wi-Fi network fingerprint as required by previous solutions [4][10][11].
- Finally our detection technique effectiveness was mathematically modeled, prototyped and evaluated in real life environment.

II. Related Work

ETA is an effective, yet simple to implement attack that targets Wi-Fi networks. To attract more customers, coffee shops and fast food restaurants tend to offer free Internet access via Wi-Fi networks. The attacker can use off the shelf Wi-Fi devices to initiate an ETA on Wi-Fi networks. Also, the attacker can stop the attack at any point of the process making such attack untraceable. [5][7].

One can think of set up VPN connection through any of the Wi-Fi APs is the panacea of ETA. Although, all the WC data traffic will be encrypted, VPN is not available for all users and have numerous points of failure [12].

ETA caught the attention of researchers for many years. The detection methods proposed so far are partial [3]. Most ETA detection methods are bound to work in very specific environments. In [3], researchers divided ETA detection into three different categories: protocol modification, hardware fingerprinting and non-hardware identification. On the other hand, [6][7] divide ETA detection into two categories: comparing data traffic at different locations of the Wi-Fi network with a known authorized list, and checking if the source of the data traffic is coming from a wireless or a wired network.

In this paper we classify ETA detection into two main categories: network administrative side, and client detection side. In network administrative side ETA detection, the network administrator will be responsible for detecting and/or assisting the WC to detect ETA. Since the network administrator will have all the information about the Wi-Fi network, he/she can have a list of fingerprints of all devices constructing the Wi-Fi network.

A fingerprint, is any information that can be used to distinguish a single device or a group of devices from one another. For example, AP hardware and location can be used as a fingerprint. In [10], AP clock skew was used as a fingerprint. Using clock skew as a fingerprint was further improved by [11]. However, without having an authorized AP list beforehand, this ETA detection will fail. Also, AP location can be used as fingerprint. On the other hand, nearby AP may trigger a false positive of an ongoing ETA. [7].

TABLE I
Notations & Acronyms

Notation	Definition
P_d	Proposed ETA detection probability
P_m	Proposed ETA detection missing probability
N	Number of recorded APs
k	Number of times attacker disconnect/connect from/to LAP
D	Time required by WC to switch between two APs
RTT	Round trip time
ETA	Evil twin attack
WC	Wireless customer
AP	Access point
LAP	Legitimate access point
RAP	Rogue access point
RWC	Rogue wireless customer
PIS	Public information server

Furthermore, the network administrative side detection will add more cost to the Wi-Fi network construction. The Network operator may have to install wireless sensors and collect traffic data at the switch/router to be compared with the available fingerprint authorized list. Another key point in this type of detection, is that the WC will still be unaware of the level of protection, (if any) that a specific Wi-Fi network is using against ETA. To sum up, administrative side ETA detection are limited, expensive and not available in many scenarios [6].

Client side ETA detection is the second category in our classification where the WC is solely responsible for detecting an ETA. This type of detection is preferred, as the WC is the one who will ensure his/her own security against ETA. In [8], the WC uses a traceroute command to display router's information between the WC and each router on the path to a certain destination. The WC executes a traceroute command to a certain destination through a random AP. Immediately, the WC switches to another AP and execute traceroute again to the same destination. If the route information using both APs are the same, then no ETA alarm will be triggered. On the other hand, if the information is not the same it means that one of the APs is RAP.

Although this ETA detection may succeed, it is vulnerable and limited. For instance, most network security administrators block traceroute commands from being executed for security purposes [13] . Additionally, traceroute uses ICMP which is vulnerable to reply attack. The attacker can store the traceroute communication between the LAP and the WC and send it to the WC when he/she connects to the RAP.

Another client side detection is based on the extra time delay added between the attacker and the LAP [6][7]. The WC connects first to one of the APs and measures the propagation delay between the WC and a nearby DNS server. Next, the WC switches to the other AP and measures the propagation delay again to the same DNS server. The extra wireless link between the LAP and the attacker will add more propagation delay compared to the direct connection of the WC to the LAP.

Although this ETA detection method is effective, it suffers from wireless signal fluctuation and traffic load on the AP that may vary the propagation delay measurements. [6].

Finally, Open WiFiHop [14] is a WC-based ETA detection that will listen to different Wi-Fi channels to capture a watermarked packet. In this paper we will address the vulnerabilities found in Open WiFiHop and present our ETA detection solution.

III. Open WiFiHop ETA detection vulnerabilities and limitation

Open WiFiHop [14] is a client side ETA detection of ETA using single ISP gateway. The detection structure is composed of a WC and a dedicated public server. First, the WC will connect to a nearby AP and send a watermarked packet to the public server. The watermarked packet is a random bit stream that is only known to the WC. After the WC sends the watermarked packet to the public server, the WC immediately switches to other Wi-Fi channels looking for any transmission of the watermarked packet. The public server will keep replying this watermarked packet to the WC. If the WC captures the watermarked packet in other Wi-Fi channels then the initial AP is RAP, else it is LAP.

Based on the procedure described above, Open WiFiHop has the following vulnerabilities and limitations.

First, open WiFiHop is vulnerable to replay attack. The public server will only reply the watermarked packet to the WC without any modification. When the WC sends the watermarked packet to the public server, the attacker can store the watermarked packet and then disconnect from the LAP. The attacker can then start sending the stored watermarked packet to the WC. Since the attacker disconnected from the LAP, no watermarked packet will be send on other Wi-Fi channels. In addition, when the WC returns back to the initial AP, the attacker can connect to the LAP. In this scenario, Open WiFiHop will fail to detect ETA.

Second, a false negative will be triggered using Open WiFiHop when the attacker gains information about the watermarked packets replay arrivals and the switching time of the public server and the WC respectively. When the WC sends the watermarked packet to the public server, he/she will immediately switch to other Wi-Fi channels looking for the watermarked packet [14]. The attacker can simply disconnect from the LAP without even replying the watermark packet since the WC is checking other Wi-Fi channels. When the WC returns back to the initial AP, the attacker can reconnect to the LAP. At this point, the WC will start receiving the watermarked packets from the public server. The attacker can also estimate when the WC returns to the initial AP simply by capturing the communication between the WC and the public server, which will pass through the attacker in the first place.

In [14], when the public server receives the watermarked packet, it will delay each reply by D time units, which is the time needed by the WC to switch form one AP to another. By measuring the time differences between two public server replies, the attacker can calculate D. Also, the WC will monitor each wireless channel by time $\geqslant (D + RTT)$ where RTT is the round trip time from the WC to the public server. RTT can be easily calculated since the initial communication between the WC and the public server went through the RAP.

In general, ETA detection security should not be based on information that can be gained, calculated and/or estimated by the attacker. In the next section we will propose an ETA detection procedure that overcomes the above vulnerabilities found in [14].

IV. Proposed ETA detection

A. Design Assumption

Our proposed detection takes advantage of the unique network architecture deployed by the first attack option of ETA using a single ISP gateway: when a WC sends/receives data through RAP, the same data will be sent/received wirelessly between the attacker's RWC and the LAP. A network administrator may extend 802.11 wireless coverage by installing more than one LAPs, however, these LAPs will be connected to network using cables.

Furthermore, our ETA detection is based on a fundamental 802.11 architecture design. When an AP fails to receive an acknowledgment response from a WC, it will assume the transmitted frame was lost due to collision or weak signal [15][16]. The AP will keep sending unacknowledged frames for a certain amount of time until it determines that the WC is offline, and then disconnects it from the wireless network.

B. Proposed Detection Design

Our ETA detection system design overcomes the vulnerabilities in WiFiHop discussed in the previous section [14]. The effectiveness of the detection procedure is not based on parameters that can be gained or estimated by the attacker. Furthermore, the ETA detection is a real-time client-side method that does not rely on trained data and/or Wi-Fi network fingerprint.

The proposed ETA system detection is composed of two parts: a WC and the public information server (PIS). First, by listening to the Wi-Fi beacon frames, the WC records the MAC address and the working Wi-Fi channel for all nearby APs that belong to the Wi-Fi network being tested. For simplicity, let us assume we have only two APs in the target Wi-Fi network, APx and APy. Wi-Fi SSID is used to determine if an AP belongs to the target Wi-Fi or not. The first step does not involve any communication between the WC and any APs (i.e., passive).

Second, the WC randomly connects to one of the recorded APs, for example APx. Once the WC is connected to APx, the Wi-Fi network DHCP assigns network configuration such as IP address to the WC. Now that the WC is connected to the Wi-Fi network, he/she establish a connection to the PIS and sends a "hello" packet. Data traffic between the WC and the PIS is encrypted. The PIS will assign a unique ID to the WC, e.g., XYZ. Such ID is capable of telling apart the communication between the WC and PIS from the communication of other WCs that may start the ETA detection at the same time in the

TABLE II
INFO PACKET DATA

Packet Seq.	WC ID	AP MAC Address
1	XYZ	APx
2	XYZ	APy
3	XYZ	APx
4	XYZ	APy

same Wi-Fi network. After the WC receives his/her ID, he/she sends APx's MAC address along with the WC's ID to the PIS. In the meantime, the WC saves the Wi-Fi network connection information. Likewise, PIS saves AP's MAC address that belongs to the connection.

Third, the WC switches randomly to other recorded APs (in our scenario is APy). At the same time, the WC changes his/her MAC address. After receiving network configuration using the new MAC address from APy, WC starts new connection to the PIS. After that, the WC sends APy's MAC address along with his/her ID to the PIS. Also, the WC saves the network configuration related to APy. In case there are more than two APs, the WC keeps repeating the previous procedure until going through the last recorded AP. As can be seen at this point, the WC is having two completely separate connections to the PIS.

Fourth, through the last connected AP (in our scenario is APy), the WC sends "Info Start" packet which signals to PIS to start sending info packets. PIS starts sending info packets to the WC through each connection separately. Info packets contain the MAC address of the AP being used to establish the connection between the PIS and the WC. Also, each info packet has increment sequence numbers to prevent replay attack, as shown in Table II.

Fifth, immediately after the WC sends info start packet, he/she randomly switches to one of the APs (APx or APy) channel and starts listening to the info packets sent by the PIS for a certain amount of time. WC filters all the incoming packets based on the WC's ID. As a result, all filtered wireless frames should have their destination MAC address pointing to one of the WC's MAC addresses. If not, then that frame was sent to a RWC. WC can then extract the MAC address inside the info packet to mark it as RAP. Also, if the WC did not receive an info packet from the AP that belongs to the listening channel, then that AP is also a RAP. Otherwise, the AP is LAP. In addition, the WC checks the sequence number of the info packets and ignores any packet with a sequence number that is less than or equal to the last one received.

Even if the attacker has all the timing information of the PIS sending interval and the WC switching/listening time, the ETA will fail because the WC's channel switching is random. The attacker cannot tell if the WC is listing to the RAP or the LAP. If the attacker stops sending info packets while the WC is listening to the RAP channel, our detection will detect the ETA. Also, if the attacker starts sending info packets while the WC is listening to the LAP Wi-Fi channel, the proposed detection will detect that the LAP is sending info packets to other WCs (attacker Wi-Fi interface). Furthermore, every info packet has its own sequence number, the attacker can't apply the replay attack on info packets.

TABLE III
DETECTION/MISSING PROBABILITY OF OUR ETA DETECTION BASED ON NUMBER OF TIMES WC MONITOR EACH RECORDED AP'S WI-FI CHANNEL

No. of Ch. Monitoring	Missing Probability	Detection Probability
1	25%	75%
2	6.25%	93.75%
3	1.5625%	98.4375%
4	0.390625%	99.609375%

At the end of the detection procedure the WC marks every recorded AP as RAP or LAP. The WC now can freely connect to any of the LAPs. The PIS deletes all the information related to the WC's ID XYZ. This makes the PIS simple to implement and maintain.

C. Proposed Detection Efficiency

In our ETA detection, the WC monitors all the recorded APs' Wi-Fi channels randomly. Given the attacker has all our ETA detection timing, he/she should decide when to disconnect/connect from the LAP to avoid being detected. Since info packets have encrypted sequence numbers, the attacker cannot save a copy and reply it to the WC. When the attacker disconnects from the LAP, he/she cannot send any info packets using the RAP. Since the WC monitors each APs' Wi-Fi channel for one time unit, the WC ETA detection missing probability P_m can be calculated as:

$$P_m = \frac{k}{N} \times \frac{N-k}{N} \tag{1}$$

where N is the number of recorded APs and k is how many times the attacker disconnect/connect from/to the LAP. The attacker's goal is to find the best value for k in order to maximize the detection missing probability P_m. This can be calculated by finding the roots of the P_m's derivative equation, which is:

$$\frac{dP_m}{dN} = \frac{N-2k}{N^2} \tag{2}$$

The roots of Equation (2) is 0 and N/2. Applying k = N/2 to Equation (1) yields $P_m = 0.25$. Given that $P_m = 0.25$, the WC's ETA detection probability P_d = 1 - $P_m = 0.75$. To increase P_d, we increased the number of times the WC monitors each recorded AP's Wi-Fi channel as shown in Table III. Monitoring each recorded AP's Wi-Fi channel for four times makes our proposed ETA detection probability $\approx 100\%$.

D. Implementation

The ETA detection WC/PIS software were implemented using C language. LORCON [17] is used to allow the WC to inject/receive frames into a Wi-Fi network. Both WC/PIS software were installed on Linux

```
Recored nearby APs info. forming target SSID
Randomly connect to one of the recorded APs
Get network conf. from DHCP server
Establish secure connection to PIS
Send "hello" pkt. to PIS
Get WC ID from PIS
Send current AP MAC Addr. and WC ID to PIS
Save connection info.
while not connected to all other recoreded APs do
    Change WC MAC Addr.
    Randomly connect to one of the remaining APs
    Get network conf. from DHCP server
    Establish secure connection to PIS
    Send current AP MAC Addr. and WC ID to PIS
    Save connection info.
end
Send "Info start" pkt. to PIS
PIS Start sending Info pkts each $D$ sec
while Each AP channel should be monitored four times do
    Randomly switch to one of the APs ch.
    Filter traffic based on WC ID
    Read all Filtered Info pkts
    if Info pkt was found then
        if Info pkt Seq. $\leq$ than previous one then
            Ignore Info pkt.
        end
        else
            if Wireless frame not sent to WC then
                Extract AP MAC addr. from info pkt
                 Mark extracted AP MAC Addr. as RAP.
            end
            else
                Ignore Info Pkt.
            end
        end
    end
    else
        Mark AP belongs to current ch. as RAP
    end
    Mark non RAP marked APs as LAP
end
```

Pseudo Code 1: Proposed ETA detection Procedure.

OS based machines. TCP protocol is used to carryout communication between the two of them. The source code for the WC/PIS software can be downloaded from https://github.com/WiFiSecurity/EvilTwinDetection.

WC starts by using LORCON to inject/receive wireless frames using Wi-Fi interface card. As soon as the WC connects to the AP, he/she starts communicating using UDP protocol with the Wi-Fi DHCP server. The Wi-Fi network DHCP server sends the network configuration to the WC. Immediately, the WC starts a connection to the PIS and receives his/her ID. We used TCP protocol to implement the communication between the WC and the PIS. Although UDP can be used to establish the connection between the WC and the PIS, TCP is preferred since it is a more reliable protocol compared to UDP. Furthermore, the data between the WC and the PIS is encrypted. Pseudo Code 1 illustrates the proposed ETA detection procedure.

V. Evaluation Procedure

We implemented a Wi-Fi network testbed to evaluate our proposed ETA detection. Wireshark software was used to monitor all communications between the WC and the PIS. Both the WC and the PIS software were installed on Kali Linux OS. The WC Wi-Fi interface card is wireless N dual-band USB adapter (TPE-NUSBDB). We assumed the attacker used D-link AC3200 Wi-Fi router to set up the RAP, and ASUS AC1900 Wi-Fi router to connect to the LAP. Where the LAP is Linksys WRT1900ACS Wi-Fi router. Figure 2 illustrates the testbed set up.

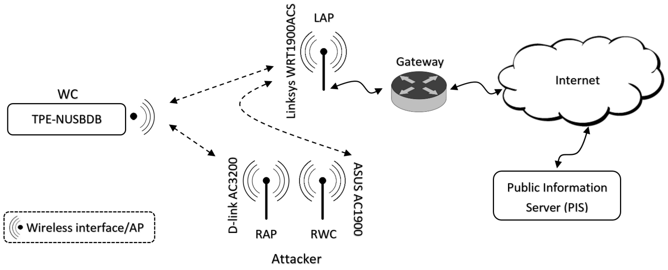

Fig. 2. Proposed ETA evaluation testbed setup.

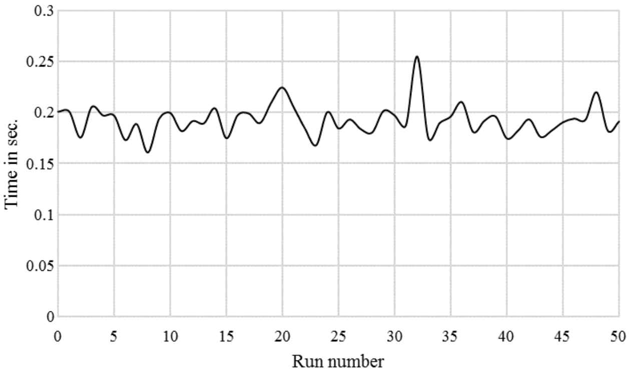

Fig. 3. WC channel switching time.

First, the WC listened to the Wi-Fi beacon and recorded the APs information such as the working channel and the MAC address. In our testbed, the WC recorded the working channels and MAC addresses of D-link AC3200 (RAP) and Linksys WRT1900ACS (LAP). After that, the WC randomly connected to one of the APs, e.g., RAP. After receiving network configuration from the DHCP server, the WC established a secured connection to the PIS and received his/her ID. Immediately, the WC sent RAP MAC address along his/her ID. The WC saved network configuration.

Second, the WC changed the Wi-Fi interface MAC address and switched to the LAP. Since the MAC address was changed, new network configuration was received from the DHCP server. The WC started a new connection to the PIS and sent LAP MAC address with his/her ID to the PIS. Now, the WC has two active connections to the PIS through both, the RAP and the LAP. Until now, the real testing has not started yet.

Our ETA detection started when the WC sent “info start” packet to the PIS. For comparison purposes, we used the same timing technique used in [14]. The PIS started sending Info

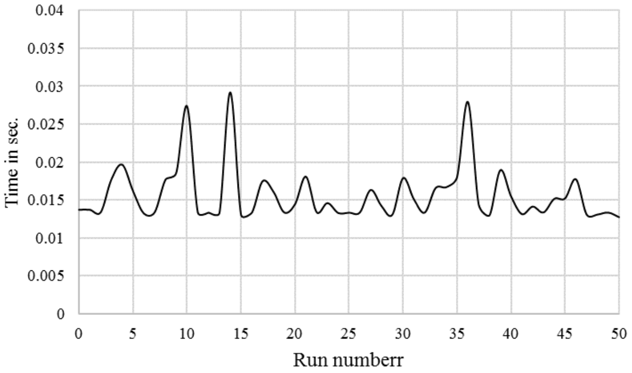

Fig. 4. Round trip time between WC and PIS.

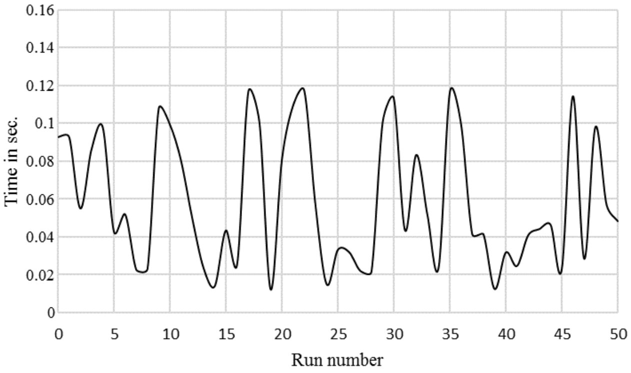

Fig. 5. Info frames average capturing time sent by LAP, RAP and RWC

packets at an interval of D seconds each, where D is the time required for the WC to switch from one AP to another. In our testbed, which was based on 50 runs, the average value of D was $\approx$ 0.2 sec with standard deviation of 0.015 sec as shown in Figure 3. Also, the WC should spend longer than $(D + RTT)$ sec to monitor each Wi-Fi channel [14], where RTT is the Round Trip Time between the WC and the PIS. Based on 50 runs, Figure 4 shows the RTT measured between the WC and the PIS which was $\approx$ 0.016 sec with a standard deviation of 0.0037 sec. As a result, the WC should monitored each Wi-Fi channel longer than (0.2 + 0.016) sec. Based on that, we chose for the WC to monitor each Wi-Fi channel for 0.4 sec. Furthermore, to avoid being affected in case the info packets were lost/dropped along the route between the PIS and the WC, the PIS continuously sends multiple info packet once in every D time.

Since each channel should be monitored four times, Equation (3) calculated our ETA detection time based on the number of APs Wi-Fi channels available in the network.

$$DetectionTime = N * (2.4) \tag{3}$$

where N is the number of Wi-Fi channels to be tested, and 2.4 is the total time to test each Wi-Fi channel which came from calculating $4 \times (0.4 + 0.2)$. Based on Equation (3), Table IV shows the detection time for all the 11 Wi-Fi channels in 802.11 b/g network.

Although WC had to wait 0.4 sec on each wireless channel, in our 50 runs, WC was able to capture LAP, RAP and RWC info packets sent by PIS in average of $\approx$ 0.06 sec with a standard deviation of 0.03 sec as shown in Figure 4 . This is due to the fact that PIS will keep sending multiple packets to the WC each time D which is equal to the switching time of the WC. By the time WC switch from one AP to another, info packets should have been already sent by the PIS and on its way to the WC.

VI. Discussion, Limitation and Future Work

In our paper, we presented an effective ETA detection of ETA using single ISP gateway. If the attacker uses his/her own broadband network connection, this ETA detection will not be effective anymore. However, combining our detection with other ETA detections of ETA using different ISP gateways, such as [5], will produce a complete detection tool that can be used to detect both ETA scenarios.

TABLE IV
Detection time based on number of channels in 802.11 b/g when every channel have one AP

No. of Channels	Detection time in sec
2	4.8
3	7.2
4	9.6
5	12
6	14.4
7	16.8
8	19.2
9	21.6
10	24
11	26.4

Our ETA detection can test all the 11 802.11 b/g WiFi channels in roughly half a minute with a detection rate close to 100%. Meanwhile, in Open WiFiHop [14], the same time was spent to test only one AP. Furthermore, our proposed detection is more secure since it was not based on parameters that can be projected by an attacker. For example, unlike Open WiFiHop [14], if the attacker has all the procedure timing information, our ETA detection efficiency will not be affected and is always approximated to 100 %.

The proposed ETA detection does not rely on train data and/or the Wi-Fi's network fingerprint, which makes it preferable for customers (such as travelers) who visit the Wi-Fi network for the first time. Furthermore, the WC will be the one who ensures his/her security. In addition, the PIS used in our ETA detection is simple to implement and maintain. No WC data will be saved on the PIS, which ensures user privacy in case the PIS was compromised.

Network administrators may extended a Wi-Fi network coverage by setting up repeaters. In general, Wi-Fi repeaters are installed in places that do not have Ethernet port. In IEEE

802.11, Wi-Fi repeater traffic uses all the four address fields in the wireless traffic frame; however, LAP, WC and RAP use only three address fields [18]. Our proposed detection can check the number of addresses used in the Wi-Fi frame to distinguish between the two types of traffic.

Finally, network administrators can protect a Wi-Fi network by using a Pre-Shared Key (PSK) Wi-Fi Protected Access (WPA) security suite [19]. These types of networks can be found in small business or home offices. If the attacker were to recover the PSK, he/she could start an ETA in a protected Wi-Fi network. For future work, we will study the current ETA detections in protected Wi-Fi networks and propose new procedure that can be used to detect an ETA in these types of Wi-Fi networks.

VII. Conclusion

In this paper, a real-time client side ETA detection of ETA using single ISP gateway was proposed. In our ETA detection, the wireless client can test the whole 11 Wi-Fi channels of 802.11 b/g network for ETA with approximately 27 seconds. No trained data and/or network fingerprint was used in the detection. Our proposed detection efficiency was mathematical modeled and implemented in real life scenario with a detection rate of $\approx 100\%$. Our proposed ETA detection can be combined with other ETA detections of ETA using different ISP gateways, such as [5], to provide comprehensive ETA detection.

References

[1] Ericsson, *"Ericsson Mobility Report"* Ericsson, Tech. Rep., June, 2015.

[2] Michael Seufert, Tobias Griepentrog, Valentin Burger and Tobias Hofeld, *"A Simple WiFi Hotspot Model for Cities"*, to be published in the IEEE Communications Letters, Dec, 2016.

[3] Fabian Lanze, Andriy Panchenko, Ignacio Ponce-Alcaide, Thomas Engel *"Hackers Toolbox: Detecting Software-Based 802.11 Evil Twin Access Points"*, IEEE 12th Annual on Consumer Communications and Networking Conference (CCNC), 225 - 232, Jan. 2015.

[4] Hossen Mustafa, Wenyuan Xu, *"CETAD: Detecting Evil Twin Access Point Attacks in Wireless Hotspots"*, IEEE Conference Communications and Network Security (CNS), 238 - 246, Oct. 2014.

[5] Omar Nakhila, Erich Dondykc, Muhammad Faisal Amjadd and Cliff Zou, *"User-Side Wi-Fi Evil Twin Attack Detection Using SSL/TCP Protocols"*, IEEE 12th Annual on Consumer Communications and Networking Conference (CCNC), 239 - 244, Jan. 2015.

[6] Chao Yang, Yimin Song, and Guofei Gu., *"Active User-Side Evil Twin Access Point Detection Using Statistical Techniques"*, IEEE Transactions On Information Forensics And Security, 1638 - 651, 2012.

[7] Chao Yang, Yimin Song, and Guofei Gu., *"Who is peeping at your passwords at Starbucks? - To catch an evil twin access point"*, IEEE Conference on Dependable Systems and Networks (DSN) , 323 - 332, 2010.

[8] Somayeh Nikbakhsh, Azizah Manaf, Mazdak Zamani, and Maziar Janbeglou, *"A Novel Approach for Rogue Access Point Detection on the Client-Side"*, IEEE 26th International Conference on Advanced Information Networking and Applications Workshops, 684 - 87, 2012.

[9] Intel.com, *"What is Wi-Fi roaming aggressiveness"*, Intel Wi-Fi Products, Aug 12, 2014.

[10] S. Jana, S.K. Kasera, *"On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews"*, IEEE Transactions On Mobile Computing, 449 - 462, March 2010.

[11] F. Lanze, A. Panchenko, B. Braatz, and T. Engel, *"Letting the Puss in Boots Sweat: Detecting Fake Access Points using Dependency of Clock Skews on Temperature,"*, Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security (AsiaCCS), 2014.

[12] Scott, Charlie, Paul Wolfe, and Mike Erwin, *"Virtual Private Networks"*, Second Edition, OReilly, 1999.

[13] Robert Sherwood, *"Discovering and Securing Shared Resources on the Internet"*, Doctor of Philosophy Dissertation, University of Maryland, 2008.

[14] Diogo Mnica, Carlos Ribeiro, *"WiFiHop - Mitigating the Evil Twin Attack through Multi-hop Detection"*, Computer Security ESORICS, Volume 6879, 21 - 39, 2011.

[15] Shravan Rayanchu, Arunesh Mishra, Dheeraj Agrawal, Sharad Saha, Suman Banerjee *"Diagnosing Wireless Packet Losses in 802.11: Separating Collision from Weak Signal"*, The IEEE 27th Conference on Computer Communications (INFOCOM), 2008.

[16] Shao-Cheng Wang, Ahmed Helmy, *"BEWARE: Background Traffic-Aware Rate Adaptation for IEEE 802.11"*, IEEE/ACM Transactions on Networking, 1164 - 1177, 2011.

[17] https://code.google.com/p/lorcon/

[18] David A. Westcott, David D. Coleman, Ben Miller, Peter Mackenzie, *"CWAP Certified Wireless Analysis Professional Official Study Guide: Exam PW0-270l"*, John Wiley & Sons, 1 edition, March 22, 2011.

[19] IEEE Standards *"IEEE 802.11w"*, 2009.